AFRICA CENTER
FOR STRATEGIC STUDIES

September 2022

CYBERSPACE AND SECURITY SECTOR GOVERNANCE IN AFRICA

ROUNDTABLE EXECUTIVE SUMMARY

On May 19-20, 2022, the Africa Center for Strategic Studies convened an expert roundtable to discuss Africa's rising cyber-related security sector governance challenges. The roundtable brought together Africa and U.S.-based practitioners and experts to discuss how to strengthen cyber security capacity while advancing democracy, the rule of law, and citizen security. This document summarizes the main points raised in these discussions, which were conducted under the not-for-attribution rule and do not necessarily reflect the view of all participants.

There was a consensus among participants that cyber capacity building initiatives need to be complemented by efforts to build institutions to ensure the transparent, accountable use of cyber-related tools. Participants offered six core insights to inform efforts by African governments, the security sector, citizens, the United States, and other external actors to improve cyber-related security sector governance:

- **Extend security sector cyber capacity building efforts beyond the development of surveillance or "offensive" capabilities, to include threat intelligence, critical infrastructure protection, and securing government communications.** The benefits of security sector involvement in cyberspace should be weighed against risks that security sector cyber authorities and capabilities diminish trust with the private sector and can be used to undermine the rights of citizens.

- **Develop legal, judicial, and other horizontal accountability mechanisms to govern the use of cyber capabilities.** Cyber and ICT-related tools are more likely to reinforce the social contract between states and citizens in countries where existing mechanisms of accountability are strong.

- **Integrate security sector cyber capacity building with broader security sector reform efforts.** Countries with ongoing SSR reform efforts should also address cyber and ICT-related policy.

- **Align cybersecurity strategy with national security strategy.** Aligning cybersecurity strategy with national security strategy will ensure that both reflect compelling national interests.

- **Expand engagement with leading technology companies.** Their control over much of the world's ICT infrastructure makes them as, if not more, influential than many states.

- **Build awareness of cyber strategy and technology policy among African security sector leaders, diplomats, and heads of state.** Leadership from senior African officials, who like their peers elsewhere are often not cyber savvy, is most needed to catalyze change.

Background and Objectives

The roundtable convened approximately 40 participants, including representatives from academia, think-tanks, civil-society, government, and security sector officials based primarily in the United States and Africa. The main objectives were to discuss: (i) how cyber-related threats are affecting Africa's security landscape; (ii) the challenges African governments and security sector actors face in responding to cyber-related threats; (iii) the implications of these responses for security sector governance across Africa; and (iv) how the US and other external actors can strengthen government and security sector capacity in a manner consistent with democracy, rule of law, and the security needs of African citizens.

The not-for attribution format allowed for participants to engage in frank, participatory dialogue on these issues over two days. The first day consisted of two sessions taking stock of African government and security sector responses to cyber-related threats and outlining how these responses have influenced the governance of the security sector. The second day consisted of two sessions to identify good practices with respect to cyber-related policy, strategy, and governance within and outside of the African security sector. The roundtable concluded with discussions of how the U.S. and other external actors can assist African states in building cyber capacity within the parameters of democratic governance.

Rising Cyber Threats, Limited Cyber Capacity

As a result of the spread of digital technology, African countries are increasingly vulnerable to a wide array of threats.[i] Participants identified six kinds of cyber-enabled enabled threats:

- **Organized Crime.** Information technology has led to new forms of cyber-enabled fraud, and has altered the networks, markets, and financing of more traditional forms of organized crime. Just one form of cyber-enabled fraud, the Business Email Compromise scam, with actors who are largely based in Africa, has caused $43 billion dollars in losses over the past five years.[ii]
- **Critical Infrastructure Sabotage.** As evidenced by the July 2021 cyberattack against Transnet, the South African port operator, Africa's critical infrastructure is becoming increasingly cyber-dependent and vulnerable to cyber-enabled sabotage.
- **Espionage.** Perhaps nowhere has the digital revolution's impact been more pronounced than in the field of intelligence. The rapid spread of surveillance platforms, open-source intelligence gathering methods, and sophisticated malware has made African states and citizens more vulnerable than ever to espionage – from without and from within.
- **Information Operations.** The rapid spread of social media has amplified misinformation, digital vigilantism, and enabled the recruitment efforts of extremist groups across the continent. External actors, such as Russia, have sponsored disinformation campaigns for political gain in dozens of countries in Africa.
- **Armed Conflict Innovation.** Information technology has accelerated general trends towards reliance on precise, automated, and intelligence-driven platforms in armed conflict in Africa and elsewhere. Over the past two decades, 'remote attacks' such as IEDs, drone strikes, and air strikes have constituted a larger and larger percentage of armed attacks.[iii]
- **Geostrategic Technology Competition.** African countries and enterprises tend to rely on external actors for much of their ICT infrastructure and technology. Participants echoed concerns that increasing technology dependence will subordinate African needs to those of external actors.

While these threats are global in character, they have unique strategic implications due to Africa's high concentration of low-income countries and rapid adoption of some digitally based technologies. For example, due to innovative companies such as Kenya's MPESA, the African region has the world's highest concentration of mobile banking. At the same time, participants highlighted how the rapid spread of mobile money, weaknesses in regulation, and low law enforcement capacity has led to significant growth in cyber-enabled fraud and crimes targeting the financial sector. A similar dynamic characterizes much of the African continent's critical infrastructure. Africa has limited cyber-dependent critical infrastructure compared to more technology dependent regions of the world, but the critical infrastructure it does have, from telecommunications networks to ports to energy grids, tend to serve large geographic areas and lack resilience and redundancy, making them 'single points of failure.'[iv]

Participants expressed particular concern with respect to the geostrategic dimensions of technology competition. African countries are dependent on foreign suppliers for most of their technology infrastructure, from undersea cables and social media platforms provided by American technology firms such as Meta to mobile phones and base stations manufactured by Huawei, the Chinese telecommunications giant. This dependence on foreign suppliers makes African users beholden to technologies at times not designed with their needs in mind. In addition, African countries fear becoming victims of cyber-enabled espionage or sabotage, particularly with respect to supply and transfer of strategically sensitive technology.

Crucially, African countries do not just face capacity deficits with respect to information technology adoption, but with respect to the policies, strategies, standards, and practices needed to govern its use. Most African countries possess neither a national cybersecurity strategy or national computer emergency response team, much less sectoral response teams needed to assess, manage, and mitigate sectoral-level cyber risk.[v] Participants noted the proliferation of cybercrime and data protection laws, but some questioned whether they were written with enough clarity and specificity to enable institutions in African countries to evolve and adapt to threats. Participants highlighted how divisions between African countries, along with an assumption prevalent among high-level policymakers and diplomats that cybersecurity is best left to technical experts, have limited African participation in UN-sponsored initiatives to examine the impact of ICTs on national security and military affairs and international declarations and treaties aimed at responding to cybercrime.

Cyberspace and Security Sector Governance Challenges

The spread of cyberspace has important implications for *security sector governance*, which can be defined as "the rules, structures, and processes of state security provision, management and oversight" pertaining to "how and why a country's security sector uses and controls force."[vi] The rising cyber-related threats African countries are facing demand changes in security provision by security sector actors. African governments, are, for example, increasingly creating police units empowered to respond to cyber-enabled crime and involved in public-private partnerships to collect and share threat intelligence. In the name of combatting threats from organized criminal networks and violent extremist groups, state surveillance and cyber espionage capabilities in Africa have rapidly expanded, as has the use of unmanned systems.

In building capacity to address cyber-enabled threats, security sector participants highlighted that they face many of the same challenges as their civilian counterparts. Security sector actors generally have low levels of cyber security awareness, particularly within the senior ranks of Africa's security sector institutions. A lack of resources and capacity has contributed to poor cybersecurity practices, such as

reliance on messaging apps including WhatsApp and Telegram to conduct sensitive law enforcement operations. Insofar as they do not rely on commercial off-the-shelf technology, African security forces depend on imported communications technology and on foreign partners to build and maintain ICT-dependent military systems. Lack of trust and poor collaboration with private sector actors who supply communications technology, logistics, and commercial-off-the-shelf platforms hinders efforts to adopt the latest technologies or protect sensitive systems.

Just as crucially, many of the changes in security provision resulting from government and security actor responses to cyber-enabled threats are undermining the accountability and oversight aspects of security sector governance. For example, some participants recognized that the rapid expansion of security sector surveillance capabilities may offer states a tactical advantage in combatting cyber-enabled threats from non-state actors. However, particularly in countries with limited oversight of the security sector, they are consistently used to undermine press freedoms, invade privacy, and stifle political opposition.

State and security sector actors have been able to acquire expanded surveillance capabilities through the acquisition of commercial malware that enable "remote-control hacking" by police, intelligence, military, and other law enforcement officials.[vii] The undermining of security sector accountability with digital surveillance tools is made possible in part by the passage of cybersecurity and cybercrime laws that expand security sector authority without requisite oversight. Often, such laws include vague definitions of cybercrime, disinformation, or hate speech that give security sector actors wide discretion in choosing whom to arrest or detain.

Participants highlighted that rising digital repression in Africa should not just be reduced to a problem of security sector overstep. Participants noted that it in some cases, it was civilian political authorities, not security institutions, that were the driving force behind the passage of laws, policies, and legal frameworks that undermine security sector accountability. In addition, some aspects of digital repression, such as the increasingly common deployment of internet restrictions or the spread of politically organized disinformation, are often not enacted by security sector officials, but by telecommunications authorities, media enterprises, or political parties.

There was a consensus among participants that digital technology is neither an unbridled force for political change and democracy, nor, alternatively, a central enabler of dictatorship. Rather, in Africa's more entrenched democracies, the adoption of digital surveillance technologies has had a less pernicious effect on governance than in Africa's authoritarian regimes, though they still require effective oversight.

This suggests that it is not capacity, but policies, strategies, and institutions that determine whether technology upholds or undermines peace, democracy, and freedom in Africa.

Participant Insights and Recommendations on African and United States Partner Response

Participants underscored the need to think creatively, and non-traditionally, about the activities, objectives, and stakeholders involved in cyber capacity building efforts. There was a consensus regarding the need for security sector stakeholders in Africa to pursue a human-centric approach to cybersecurity and engaging in multistakeholder cooperation in service of this approach. This requires that the building of technical capabilities in threat detection, incident response, and offensive cyber capabilities be complemented by efforts to build transparent and accountable institutions that govern how African governments and security sector officials employ cyber-related tools.

Participants offered six core insights aimed at enabling governments, security sector actors, the private sector, and civil society in Africa to build cyber capacity and support democratic governance:

1. **Focus security sector cyber capacity building efforts beyond the development of surveillance capabilities.** Within African security and defense sectors, a major focus of cybersecurity capacity building efforts has been the development of intelligence, surveillance, and reconnaissance (ISR) capabilities. Participants highlighted the need to improve cyber capacity beyond ISR, to include:
    - collection, sharing and publication of threat intelligence,
    - the defense of government and military information networks,
    - cyber incident management and response,
    - the development of reliable, secure, and interoperable communications systems,
    - the identification and protection of critical information infrastructure,
    - the use of ICT to enable military operations.

    The non-traditional nature of cyberspace requires careful thinking about defense and security sector roles and responsibilities. Security sector actors will need to overcome tendencies towards classification and secrecy to ensure that they are able to encourage open communication, collaboration, and trust across a range of stakeholders responsible for cybersecurity. For example, "a telecom's technical staff might be much better and more cost effective at identifying, addressing, and resolving cybersecurity threats than a national security operative, particularly at the tactical level."[viii] The wealth of expertise and human capital in the private sector means that it is usually in a better position to respond to incidents that affect the infrastructure they manage, but industry can benefit from government and security sector efforts to coordinate and share information.

2. **Link security sector cyber capacity building with broader security sector reform and governance efforts.** Participants emphasized that cybersecurity capacity building efforts should adopt a human-centric rather than a regime-centric approach. This requires linking cyber capacity building with broader security sector reform and governance efforts. Cybersecurity capacity building should be sensitive to the second and third order consequences these efforts might have with respect to the formal and informal processes through which security forces deliver public goods and services to citizens. Capacity building that enhances monitoring and surveillance capabilities of security sector actors without adequate means to ensure they are used accountably risk doing more harm than good.

3. **Expand cybersecurity capacity building efforts to include the development of legal, judiciary, and horizontal accountability.** Participants highlighted how cyber capabilities tend to be used far less repressively in African countries with more robust democratic institutions. Therefore, an essential component of cyber-related capacity building needs to extend beyond the military and police, and include the development of legal, judiciary, and institutional frameworks to ensure that cyber capabilities are used transparently and accountably. In tandem with traditional cyber capacity building efforts, there is a need to strengthen executive oversight mechanisms such as inspector generals and ombudsmen, develop more precisely defined and targeted cybersecurity laws, and reduce the use of shutdowns and restrictions that cut off online speech and communications for large groups of people.

4. **Integrate cybersecurity strategies with national security strategies.** Participants highlighted how cybersecurity strategies across Africa need to be more closely linked to national security strategies. Just as security sector actors play an important role in development and implementing national

cybersecurity policy and strategy, cyber-related threats and challenges from state and non-state actors are of increasing concern. Given this rising significance, cyber-related threats and the security sector's roles and responsibilities in mitigating them should be addressed as part of national security strategy design, development, and implementation.

5. **Expand engagement with leading technology companies.** Participants highlighted the need for government and security sector actors to become more engaged, within the parameters of robust checks and balances, with leading technology companies such as Google, Microsoft, Meta, and Huawei. They operate much of the world's internet architecture, are on the forefront of responding to systemic cyber risks, and possess resources and expertise that governments do not. Perhaps more than any one stakeholder, they are best positioned to ensure reliable and secure internet access for government, security sector, and citizen end users. Pro-active efforts are needed both by leading technology companies, who are often unaware or unresponsive to how their platforms are used as vectors of cyberattack or to spread misinformation and hate speech, and by government and security sector actors, who are at times among the main perpetrators of such abuses and often manipulate technology platforms to coopt or repress citizens, the media and the opposition. Civil society organizations in particularly might be best positioned to foster productive dialogue between key public and private sector stakeholders.

6. **Build cyber awareness among African security sector leaders, diplomats, and heads of state.** Observing how cyber capacity building efforts in Africa are driven by the technical experts, civilian ministries, and mid-level uniformed cyber or ICT officers, participants identified three main government actors that could benefit from training and awareness raising with respect to the strategic implications of the spread of information technology for their fields. First, security sector leaders could benefit from enhanced awareness of how digital technology is influencing threats from organized actors with significant coercive capabilities such as states, organized criminal networks, and violent extremist groups. Second, more diplomats trained in the nuances of cyber diplomacy, norms, and state behavior in cyberspace would enable African states to represent their countries more effectively in high-level fora. Finally, given the growing strategic significance of cyberspace, it is imperative that African heads of state immerse themselves in mitigating the risks, as well as harnessing the benefits, of expanding information technology.

---

[i] Nate Allen, "Africa's Evolving Cyber Threats," Africa Center for Strategic Studies, January 19, 2021, https://africacenter.org/spotlight/africa-evolving-cyber-threats/

[ii] Federal Bureau of Investigation, "Business Email Compromise: The $43 Billion Scam," Public Service Announcement, May 4, 2022, https://www.ic3.gov/Media/Y2022/PSA220504

[iii] Africa Center for Strategic Studies, "Violent Conflict Trends," Emerging Security Sector Leaders Program, June 9, 2022, https://www.youtube.com/watch?v=GLSsiNZoeuk&feature=emb_logo

[iv] Nathaniel Allen and Noëlle van de Waag-Cowling, How African States can Tackle State-backed Cyber Threats, *Brookings: Tech Stream*, 15 July 2021, https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/.

[v] For comprehensive data, see Information Technology Union, Global Cybersecurity Index, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[vi] Geneva Center for Security Sector Governance (DCAF), *Security Sector Governance: Applying the Principles of Good Governance to the Security Sector*, DCAR SSR Backgrounder 2017, p. 4, https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security%20Sector%20Governance_0.pdf

[vii] Bullelani Jili, "The Spread of Surveillance Technology in Africa Stirs Security Concerns," Africa Center for Strategic Studies, " December 11, 2020, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns

[viii] Abdul Hakeem Ajijola, quoted in Africa Center for Strategic Studies, "National Cybersecurity Strategy," Virtual Academic Program on Cyberspace Security Priorities for Africa's National Security Actors, 17 August 2021, https://youtu.be/Rlf6AVYuSns?t=610